Information-theoretic interpretation of quantum error-correcting codes

Nicolas J. Cerf[1,3] and Richard Cleve[2,3]
[1] *W. K. Kellogg Radiation Laboratory, California Institute of Technology, Pasadena, California 91125*
[2] *Department of Computer Science, University of Calgary, Calgary, Alberta, Canada T2N 1N4*
[3] *Institute for Theoretical Physics, University of California, Santa Barbara, California 93106*
(February 1997)

Quantum error-correcting codes are analyzed from an information-theoretic perspective centered on quantum conditional and mutual entropies. This approach parallels the description of classical error correction in Shannon theory, while clarifying the differences between classical and quantum codes. More specifically, it is shown how quantum information theory accounts for the fact that "redundant" information can be distributed over quantum bits even though this does not violate the quantum "no-cloning" theorem. Such a remarkable feature, which has no counterpart for classical codes, is related to the property that the ternary mutual entropy vanishes for a tripartite system in a pure state. This information-theoretic description of quantum coding is used to derive the quantum analogue of the Singleton bound on the number of logical bits that can be preserved by a code of fixed length which can recover a given number of errors.

PACS numbers: 03.65.Bz,89.70.+c KRL preprint MAP-209

I. INTRODUCTION

The potential use of quantum computers for solving certain classes of problems has recently received a considerable amount of attention (for a review see, *e.g.*, [1–3]). A major obstacle in the building of quantum computers, however, is the coupling of the computer with its environment or the *decoherence*, which rapidly destroys the quantum superposition at the heart of quantum algorithms. An essential element in the realization of such quantum computers is therefore the use of quantum error-correcting codes, which have been shown to ensure protection against decoherence [4–14]. Quantum codes are similar in many respects to classical codes. In classical coding theory, logical words (of k bits) are encoded into codewords (of $n > k$ bits). The latter are suitably chosen among the set of all 2^n possible words of n bits so that the alteration because of noise of say t bits (at most) can be recovered. A specific set of codewords then constitutes an $[n, k, t]$ code, encoding k bits into n bits and correcting all patterns of t (or fewer) errors among those n bits. The simplest example of a classical code with $k = 1$, $n = 3$, and $t = 1$ is the repetition code where a logical bit 0 (or 1) is encoded into 000 (or 111); decoding is simply performed using the majority rule, which is enough to recover $t = 1$ errors. In classical coding theory, corrupted data is thus restored by introducing redundancy ($n > k$), that is by duplicating part of the information that must be preserved. (In the above—very inefficient—example, information is triplicated.) In quantum coding theory, the central issue is to find a set of 2^k quantum codewords (of n qubits) such that *quantum information* can be protected against the alteration due to coupling with an environment (*i.e.*, such that the quantum system survives decoherence). At first sight, it seems that, since the duplication of an arbitrary quantum state is forbidden by the quantum *no-cloning* theorem [15], "quantum redundancy" is impossible. However, after the pioneering work of Shor [4], it has been realized that quantum coding is achievable in spite of the no-cloning theorem, and a great deal of work has recently been devoted to this issue [5–14]. It has been shown that quantum information can be distributed over many qubits through a suitable encoding and subsequently recovered after partial alteration, without violating the no-cloning theorem.

In this paper, we aim at clarifying some aspects of quantum coding from a perspective centered on quantum entropies. It has been shown recently that classical and quantum entropies can be described within a unified information-theoretical framework involving negative conditional entropies [16,17], as briefly outlined in Appendix A. Here, we apply this framework to quantum error-correcting codes, paralleling the classical description of error correction in Shannon theory. We show that, for an arbitrary entanglement between the logical words and a "reference" system to be preserved, the quantum *mutual* entropy between this "reference" and any "interacting" part of the codewords must be vanishing prior to decoherence. In other words, an entropic condition for perfect quantum error correction is that the "reference" system is statistically *independent* of any arbitrarily chosen part of the codewords that might interact with the environment. This condition relies on the conservation of quantum mutual entropies implied by unitarity, along with the property of strong subadditivity of quantum entropies (see Appendix A). It expresses the fact that the environment cannot become *directly* entangled with the "reference" system (entanglement may arise only via the codewords), or, roughly speaking, that the environment cannot extract information about the logical words.

We continue by deriving the analogue of the Singleton bound for quantum codes [11], *i.e.*, $k \leq n - 4t$, using simple arguments based on this entropic approach. Such an information-theoretic description of coding sheds new light on the interpretation of this bound in terms of "weak" cloning. While the quantum bits that are altered as a result of any error are statistically independent of the reference (or the encoded logical word), the quantum information stored in the entire codeword remains unaffected. This results from the fact that the *ternary* mutual entropy vanishes for any entangled tripartite system in a pure state, a property which has no classical counterpart [17]. The central point is that, in contrast with classical codes, no duplicating—or full cloning—is achieved by *quantum* error-correcting codes. Rather, a "weak" quantum cloning is achieved, such that any part of the codeword susceptible to decohere appears independent of the reference although the entire codeword remains entangled with it. This purely quantum situation is forbidden in classical information theory due to the non-negativity of Shannon conditional entropies, and reflects a fundamental difference between classical and quantum error correcting codes.

II. QUANTUM ERROR CORRECTION

Let us consider a set of orthogonal logical states $|i_L\rangle$ (with $i = 1, \cdots 2^k$) which are encoded into orthogonal codewords $|i_Q\rangle$ consisting of n qubits. (The index Q refers to the quantum channel on which the codewords are sent.) The states $|i_L\rangle$ belong to the logical Hilbert space $\mathcal{H}_L$ of dimension $d_L = 2^k$ spanned by the k logical qubits, while the states $|i_Q\rangle$ belong to $\mathcal{H}_Q$ of dimension $d_Q = 2^n$. We have clearly $d_Q > d_L$, which is the quantum equivalent of classical "redundancy": the logical states are encoded in some 2^k-dimensional subspace of the full 2^n-dimensional Hilbert space so that part of the information in the n qubits is "redundant". Qualitatively speaking, $n - k$ qubits of the codewords represent redundant information (they are equivalent to the "check bits" of classical codes [18]). In Section IV, we will make this concept of quantum "redundancy" more quantitative.

The key property of a quantum code lies in its ability to protect an *arbitrary* superposition of logical states $\sum a_i|i_L\rangle$ against decoherence. Equivalently, a quantum code is such that the entanglement of the k logical qubits with a "reference" system R is preserved against decoherence. In fact, this description of quantum coding as a mean to transmit (or conserve) entanglement with respect to R in spite of the interaction with an environment is more convenient for our information-theoretic description and will be adopted in the following. Accordingly, we start by considering the initial entangled state

$$|\psi_{RL}\rangle = \sum_{i=1}^{2^k} a_i|i_R\rangle|i_L\rangle \tag{2.1}$$

where R and L refer to the reference and logical states, respectively. (This is the Schmidt decomposition of a pure entangled state.) We then consider the transformation of $|\psi_{RL}\rangle$ due to encoding followed by decoherence. Encoding is performed by use of a unitary transformation that maps the states $|i_L\rangle|0\rangle$ to the codewords $|i_Q\rangle$, where $|0\rangle$ stands for the initial state of the $n-k$ auxiliary qubits (or check bits). Thus, after encoding, the joint state of the reference R and the quantum channel Q is

$$|\psi_{RQ}\rangle = \sum_{i=1}^{2^k} a_i|i_R\rangle|i_Q\rangle \tag{2.2}$$

It is a pure state of vanishing entropy $S(RQ) = 0$; the quantum entropies of R and Q are $S(R) = S(Q) = H[a_i]$, where H stands for the Shannon entropy,

$$H[a_i] = -\sum_i |a_i|^2 \log |a_i|^2 \, . \tag{2.3}$$

Let us suppose now that the codewords are sent on a noisy quantum channel in which they suffer decoherence due to an environment E. Following Schumacher's model of a noisy channel [19], we assume that the environment is initially in the pure state $|0\rangle$ and then interacts with the channel according to the unitary transformation U_{QE}, so that the joint state of the entire system becomes

$$|\psi_{R'Q'E'}\rangle = (1_R \otimes U_{QE}) \sum_{i=1}^{2^k} a_i|i_R\rangle|i_Q\rangle|0\rangle \tag{2.4}$$

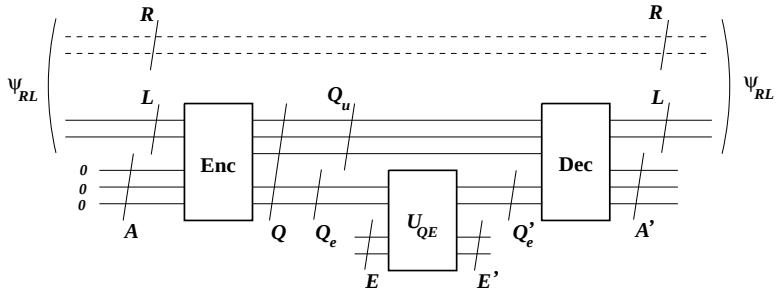
(The prime refers to the systems *after* decoherence.) This noisy channel is pictured in Fig. 1 and will be the basis of our description of quantum coding in terms of quantum entropies. More specifically, we will consider a "deterministic" error model in which the position of the erroneous bits is *known*, usually referred to as the quantum *erasure* channel [13]. In this channel, the decoherence induced by the environment involves e qubits at known locations, *i.e.*, e erasures. The component Q_e (of e qubits) of the codeword interacts with E (suffers e erasures), while the rest Q_u (of $n - e$ qubits) is left unchanged by this interaction. Accordingly, the unitary transformation in Eq. (2.4) is of the form

$$U_{QE} = 1_{Q_u} \otimes U_{Q_e E} \tag{2.5}$$

As an example, we can suppose that the environment is made of e qubits initially in a $|0\rangle$ state and that $U_{Q_e E}$ effects the exchange between these qubits and the e qubits of Q_e (a reversible operation). As a result, the qubits of Q_e are erased (reset to $|0\rangle$) while the qubits of E get the original value of the erased qubits. As the environment is traced over in order to determine the state of

the channel Q after decoherence, quantum information is apparently erased even though the overall process is unitary. Of course, any other $U_{Q_e E}$ could result from decoherence, and a quantum erasure-correcting code will be such that the entanglement with R is preserved for an arbitrary $U_{Q_e E}$.

FIG. 1. Schematic model of a noisy quantum channel preceded by encoding and followed by decoding. The logical states (system L of k qubits) are entangled with the reference system R. Encoding, using an ancilla A of $n-k$ "check" qubits initially in a $|0\rangle$ state, yields the codewords (system Q of n qubits). Then, e qubits (Q_e) are "erased" by interacting with the environment E via U_{QE}, while the $n-e$ remaining ones (Q_u) are unchanged. Decoding, involving the "erased" qubits Q'_e along with the unchanged ones Q_u yields the k logical bits L in the initial entangled state ψ_{RL} with the reference R. The primes refer to the systems after environment-induced decoherence.



Before discussing coding and decoherence using quantum entropies (Section IV), let us first review some basics of quantum error-correcting codes. It is known that, rather than coupling the codewords with an environment, one can model the errors by use of error operators E. For the purpose of error correction, it is enough to consider errors of the type σ_x (bit-flip), σ_z (phase-flip), and σ_y (bit- and phase-flip), since, by linearity, a code that can correct these errors can correct arbitrary errors [7]. For a $[n,k,t]$ code, *i.e.*, a code correcting t errors at most, the error operators E applied on the codewords are of the form $1^{\otimes(n-t)} \otimes E^{\otimes t}$, *i.e.*, the tensor product of the identity on $n-t$ qubits and t one-bit error operators on the altered qubits. The one-bit error operators are any linear combinations of the algebra basis $\{1, \sigma_x, \sigma_y, \sigma_z\}$. It has been shown by Knill and Laflamme [11] that a necessary and sufficient condition on quantum error-correcting codes is that

$$\langle i_Q|E_a^\dagger E_b|i_Q\rangle = \langle j_Q|E_a^\dagger E_b|j_Q\rangle \tag{2.6}$$
$$\langle i_Q|E_a^\dagger E_b|j_Q\rangle = 0 \qquad \text{for } i \neq j \tag{2.7}$$

where the $|i_Q\rangle$ and $|j_Q\rangle$ are any two codewords and E_a, E_b are chosen from the set of t-error operators defined above. Conditions (2.6) and (2.7) can be understood by considering the decoding operation as an "inverse" unitary transformation [14] that maps the n qubits of the corrupted codeword Q' into k qubits (the original logical word L) and $n-k$ check qubits (the ancilla A'), as represented in Fig. 1. Considering the action of decoding on two codewords $|i_Q\rangle$ and $|j_Q\rangle$ that have been corrupted by errors E_a or E_b, it can be shown that the state in which the ancilla is left cannot depend on the logical state, that is the decoding must be such that

$$\begin{aligned} E_a|i_Q\rangle &\to |i_L\rangle \otimes |A_a\rangle \\ E_b|i_Q\rangle &\to |i_L\rangle \otimes |A_b\rangle \\ E_a|j_Q\rangle &\to |j_L\rangle \otimes |A_a\rangle \\ E_b|j_Q\rangle &\to |j_L\rangle \otimes |A_b\rangle \end{aligned} \tag{2.8}$$

In other words, the final state of A must be the same for both codewords $|i_Q\rangle$ and $|j_Q\rangle$, and depend only on the error syndrome a or b. This condition is clearly required in order to recover an initial *arbitrary* superposition $\sum_i a_i|i_L\rangle$ (*i.e.*, the ancilla must be in a tensor product with the k logical qubits after decoding). Conditions (2.6) and (2.7) then result straightforwardly from the orthogonality of the logical states $|i_L\rangle$ and $|j_L\rangle$, and the conservation of scalar products by unitarity.

The above considerations also apply to the quantum *erasure* channel in which the position of the e erroneous bits is *known* [13]. Note that conditions (2.6) and (2.7) obviously correspond to the case where the errors are applied at t *unknown* positions in the codeword. Clearly, if the error-correcting code aims at correcting for *erasures* only, the error operators E_a and E_b differ from each other by one-bit error operators at the *same* positions only. Therefore, as the product of two such e-erasure operators is another e-erasure operator (a linear combination of the E_a's), the necessary and sufficient condition for erasure-correction becomes [13]

$$\langle i_Q|E_a|i_Q\rangle = \langle j_Q|E_a|j_Q\rangle \tag{2.9}$$
$$\langle i_Q|E_a|j_Q\rangle = 0 \qquad \text{for } i \neq j \tag{2.10}$$

It results that an error-correcting code correcting t errors (at unknown positions) is equivalent to an e-erasure correcting code with $e = 2t$. This equivalence will be very

useful in the following because the quantum erasure channel is easier to treat using an entropic approach. Before coming to the information-theoretic analysis of quantum error-correcting codes (Section IV), let us first analyze classical error correction in terms of entropies. This will make the classical-quantum correspondence more transparent.

III. ENTROPIC CONDITION FOR CLASSICAL ERROR/ERASURE CORRECTION

Just like in the quantum case, one can define two classes of classical noisy channels, depending on the fact that the errors occur at known or unknown locations. In the former case, the located errors are called *erasures*, and an erasure-correcting code is such that, if e bits out of the n bits are "erased", it is possible to recover the encoded logical word from the $n-e$ remaining bits only [20]. In the latter case of classical codes capable of correcting t errors at unknown positions in codewords of size n, all the n bits of the corrupted codewords must be used in the decoding operation. Exactly as for quantum codes, it is easy to show that a classical code can correct t errors at unknown locations if and only if the same code can correct $e = 2t$ erasures at known locations. The proof is as follows. Let us consider two codewords of length n, w_i and w_j, and two error strings, e_a and e_b (the bits in a codeword are flipped where the corresponding bits in the error string are equal to 1). To be able to recover t errors, we must have

$$w_i \oplus e_a \neq w_j \oplus e_b \tag{3.1}$$

for any two codewords and for all possible error strings having t bits (or fewer) equal to one. Here, $\oplus$ is the bitwise addition modulo 2 and $\neq$ means that the two strings must differ by at least one bit. A classical code correcting t errors must therefore be such that the distance between any two codewords is larger than or equal to $2t+1$, since the error strings e_a and e_b can have at most t bits equal to one, implying that $e_a \oplus e_b$ can have at most $2t$ bits equal to one. Now, in the case of codes capable of correcting e erasures, the positions of the bits equal to one in e_a and e_b are identical, so that $e_c \equiv e_a \oplus e_b$ can have at most e (rather than $2e$) bits equal to one and is therefore another e-error string just as e_a or e_b. Thus, the condition for recovering e erasures is

$$w_i \oplus e_c \neq w_j \tag{3.2}$$

In other words, the distance between any two codewords must only be larger than or equal to $e + 1$. Obviously, Eq. (3.1) parallels Eqs. (2.6-2.7), while Eq. (3.2) parallels Eqs. (2.9-2.10). The resulting equivalence $e = 2t$ will be important for our concern because the entropic analysis is more adapted to erasure correction.

Let us shortly describe coding in the case of a classical erasure channel [20]. We consider encoding as a classical channel whose input X is made of k logical bits and output Y is made of n physical bits (the codewords). We assume that the set of logical words x_i occur with probability p_i, so that the entropy of the input X is

$$H(X) = -\sum_i p_i \log p_i \tag{3.3}$$

The input X can be recorded (a classical variable can be "cloned") and thus compared with the output Y. As the encoding is reversible (it is a one-to-one mapping), the mutual entropy is conserved through encoding, that is

$$I \equiv H(X{:}Y) = H(X{:}X) = H(X) \tag{3.4}$$

where I is defined as the mutual entropy (or information) between input and output that must be preserved in the classical erasure channel. Let us assume that Y is split into e erased bits, Y_e, and $n - e$ unchanged bits, Y_u. (The position of the erased and unchanged bits is known.) The condition for classical erasure correction is clearly that the uncertainty of the input when the $n - e$ unchanged bits are known vanishes, that is

$$H(X|Y_u) = 0 \ . \tag{3.5}$$

In other words, this means that the e bits can be erased without preventing the ability of inferring the input X from Y_u without error. Since we have $H(X|Y) = H(X|Y_eY_u) = 0$ as a result of Eq. (3.4), *i.e.*, it is obviously possible to infer X from $Y \equiv Y_eY_u$, we obtain the basic entropic condition for classical error correction

$$H(X{:}Y_e|Y_u) = H(X|Y_u) - H(X|Y_eY_u) = 0 \tag{3.6}$$

Physically this expresses that, conditionally on the $n - e$ unchanged bits, no information about X is lost in the e erased bits. Classical coding works because the $n - e$ unaffected bits contain the entire information I about X, that is

$$H(X{:}Y_u) = H(X{:}Y) = I \ , \tag{3.7}$$

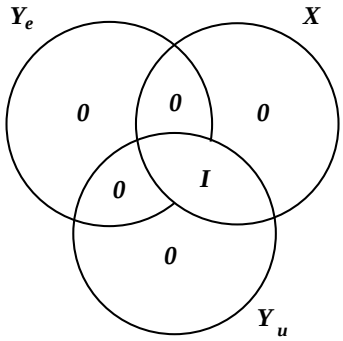
so that the e bits that are erased are "redundant". Using the chain rule for Shannon mutual entropies,

$$H(X{:}Y_eY_u) = H(X{:}Y_u) + H(X{:}Y_e|Y_u) \tag{3.8}$$

it is clear that Eq. (3.7) is satisfied if and only if the condition Eq. (3.6) is satisfied. In an erasure-correcting code, the k bits of information are thus distributed among the n bits of Y in such a way that condition Eq. (3.6) is satisfied for any splitting of the n bits into e erased and $n-e$ unchanged bits. The general classical entropy diagram corresponding to this situation is represented in Fig 2. The condition for erasure correction, Eq. (3.6), appears

in this Figure as the vanishing entropy shared by X and Y_e, but *not* by Y_u.

FIG. 2. Entropy diagram for a classical erasure-correcting code. The input X stands for the logical bits, while the output Y (the codewords) is split into the erased bits Y_e and the unchanged bits Y_u. The condition for erasure-correction is $H(X{:}Y_e|Y_u) = 0$, that is the entire information must be found in the unchanged bits, $H(X{:}Y_u) = I$.



Let us briefly show that, for a classical code, it is impossible that *all* the patterns of e "erasable" bits are independent of X, *i.e.*, do not contain some *redundant* information about X. (This feature turns out to be possible for a quantum code, as shown in Section IV.) Suppose that we could isolate two subparts of Y *independent* of X, that is two patterns of bits, say Y_1 and Y_2, such that

$$H(X{:}Y_1) = H(X{:}Y_2) = 0 \tag{3.9}$$

Suppose also that, taken together, Y_1 and Y_2 provide the entire information about X, that is

$$H(X{:}Y_1Y_2) = I \tag{3.10}$$

This should be the case if we want to make a set of bits that fully determines X (such as Y_u) out of pieces that are independent of X. We have

$$\begin{aligned} H(X{:}Y_1) + H(X{:}Y_2) &= H(X{:}Y_1Y_2) + H(X{:}Y_1{:}Y_2) \\ &= I + H(Y_1{:}Y_2) - H(Y_1{:}Y_2|X) \end{aligned} \tag{3.11}$$

Since the logical word X fully determines any bit of the codeword Y, we have $H(Y_1{:}Y_2|X) = 0$. Thus, the subadditivity of entropies, $H(Y_1{:}Y_2) \geq 0$, implies that

$$H(X{:}Y_1) + H(X{:}Y_2) \geq I \tag{3.12}$$

which is incompatible with Eq. (3.9) if $I > 0$. One of the subpart (Y_1 or Y_2) must necessarily be correlated with X (have a non-vanishing mutual entropy with X) if the other one is independent of X. Some pattern of e "erasable" bits, including Y_1 or Y_2, will therefore be redundant (contain some information about X that is already in Y_u) as a consequence of strong subadditivity.

IV. ENTROPIC CONDITION FOR QUANTUM ERROR/ERASURE CORRECTION

A. Classical correspondence

The above information-theoretic analysis can be straightforwardly applied to the case of a quantum erasure-correcting code. Here, the reference R plays the role of the input X, while Q (the quantum codewords) replaces the output Y. We also substitute the classical notion of Shannon mutual entropy (information) between X and Y with the quantum notion of von Neumann mutual entropy between R and Q, and use the extension to the quantum regime of the fundamental relations between Shannon entropies in a multipartite system [16,17,21] (see Appendix A). First, the mutual entropy between the logical words L and R is conserved through encoding (since it is unitary), so that we have

$$I_q \equiv S(R{:}Q) = S(R{:}L) \tag{4.1}$$

for the mutual entropy between the codewords Q and R. Here, I_q can be seen as the "quantum information" (the entanglement with R) which must be preserved in the quantum erasure channel. As before, we assume that Q is split into Q_e (the e erased qubits) and Q_u (the $n-e$ unchanged qubits). Just like in the classical case, it is intuitively clear that entanglement is preserved at the condition that the total mutual entropy with R is found in the unaffected qubits, Q_u, that is

$$S(R{:}Q_u) = S(R{:}Q) = I_q \tag{4.2}$$

in analogy with Eq. (3.7). Using the chain rule for the quantum mutual entropy between R and $Q \equiv Q_eQ_u$,

$$S(R{:}Q_eQ_u) = S(R{:}Q_u) + S(R{:}Q_e|Q_u) \tag{4.3}$$

we conclude that the condition for quantum erasure correction is

$$S(R{:}Q_e|Q_u) = 0 \tag{4.4}$$

the straightforward analogue of Eq. (3.6). At this point, the parallel with classical erasure correction breaks down because of a peculiar property of quantum entropies. It is shown in Ref. [17] that the *ternary* mutual entropy of any entangled tripartite system in a pure state vanishes (see also Appendix A). In the case of interest here, the tripartite system RQ_eQ_u is in the pure state $|\psi_{RQ}\rangle$, so that we have $S(R{:}Q_e{:}Q_u) = 0$. As a consequence, we obtain from Eq. (4.4) the basic entropic condition for quantum erasure correction

$$S(R{:}Q_e) = S(R{:}Q_e|Q_u) + S(R{:}Q_e{:}Q_u) = 0 \tag{4.5}$$

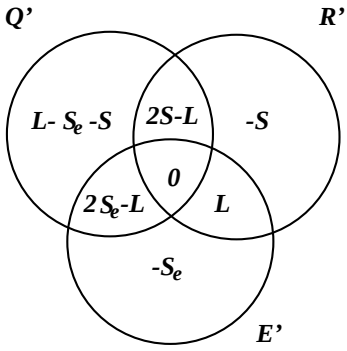
Physically, this expresses that the "erased" part of the codewords Q_e must be *independent* of the reference R. This is very different from the classical situation, where,

in order to enable erasure correction, the erased bits must by construction be correlated with X. In other words, "classical redundancy" requires correlation of the e redundant bits with X, while "quantum redundancy" is achieved *without* correlating (or entangling) the erased qubits with R. We will show later on that the above entropic condition, Eq. (4.5), can be derived more rigorously, using the property of strong subadditivity of quantum entropies and the entropic condition for perfect quantum error correction [19,21].

B. Quantum loss of a noisy channel

As explained in Section II, we assume that the codewords sent on the quantum noisy channel suffer an arbitrary decoherence due to the environment E, that is U_{QE} is an arbitrary unitary transformation. (We do not restrict ourselves to a quantum erasure channel for the moment.) After such an an arbitrary environment-induced decoherence, the joint system $R'Q'E'$ is in the state $|\psi_{R'Q'E'}\rangle$ given by Eq. (2.4). The corresponding quantum entropy diagram is represented in Fig. 3 (as mentioned earlier, the primes refer to the systems *after* decoherence).

FIG. 3. Entropy diagram summarizing the entropic relations between the entangled systems Q' (quantum channel), R' (reference), and E' (environment) after decoherence (see also Ref. [21]).



As shown in Ref. [21], it depends on three parameters, $S = S(R') = S(R)$, the entropy of the reference R (which is also equal to the entropy of Q before decoherence), $S_e = S(E')$, the entropy of the environment after decoherence, and[1]

$$\begin{aligned} L &= S(R'{:}E'|Q') \\ &= S(R'Q') + S(E'Q') - S(Q') - S(R'Q'E') \\ &= S(E') + S(Q) - S(Q') \,, \end{aligned} \tag{4.6}$$

the *loss* of the channel (following the terminology of Shannon theory [18]). The quantum loss L can be shown to be the analogue of the loss in a classical noisy channel, and thus can be written as a quantum conditional mutual entropy, *i.e.*, the quantum mutual entropy between R' and E', conditionally on Q' [21].

The loss L has a simple physical interpretation in the case of a *classical* noisy channel: it corresponds to the entropy of the input X of the channel conditional on its output Y, *i.e.*, $L = H(X|Y)$, thereby characterizing the unavoidable uncertainty in the decoding operation (when inferring the input from the corrupted output). Equivalently, it corresponds to the mutual entropy between the input and the environment, conditional on the output, *i.e.*, $L = H(X{:}E|Y)$. That is, for a given output, L measures the information about the input that has been irrecoverably lost in correlations with the environment. If X corresponds to encoded codewords and Y to corrupted ones due to a particular error source, the condition $L = 0$ must be satisfied for the error-correcting code to preserve the codewords against classical noise [18].

In Ref. [21], it is shown that the same interpretation holds for the quantum loss L, substituting the classical notion of mutual information between X and E (conditional on Y) with the quantum notion of von Neumann mutual entropy between R' and E' (conditional on Q'). The reference R $(= R')$ plays the role of the input X, while Q' replaces the output Y. Accordingly, it is expected that a vanishing quantum loss corresponds to a situation where decoherence can be entirely eliminated using a quantum code. Indeed,

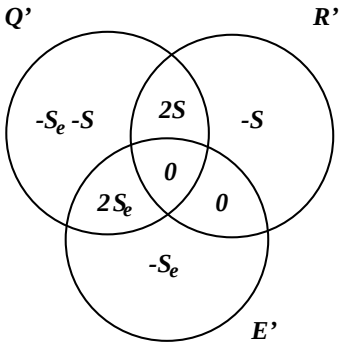
$$L = S_e + S - S(Q') = 0 \tag{4.7}$$

is a necessary and sufficient condition for the existence of a perfect quantum error-correcting code, as proven recently by Schumacher and Nielsen [19]. In Fig. 4, the entropy diagram of $R'Q'E'$ is represented in the case where this condition is achieved. It appears that, when $L = 0$, the state of Q' becomes entangled *separately* with the environment ("bad" entanglement) and the reference ("good" entanglement), allowing this "bad" entanglement to be transfered to an ancilla (the $n-k$ check qubits) while recovering only the "good" one. This transfer of entanglement, requiring a local action on Q only (not on E), can be seen as a measurement of the error

[1] Since the total system $R'Q'E'$ is in a pure state after decoherence, *i.e.*, $S(R'Q'E') = 0$, its Schmidt decomposition implies $S(R'Q') = S(E')$ and $S(E'Q') = S(R')$, resulting in the last relation in Eq. (4.6).

syndrome (the ancilla becoming entangled with E) leaving the original state intact.

FIG. 4. Entanglement between Q', R', and E' in a lossless ($L = 0$) quantum channel. The quantum system Q' is entangled "separately" with R' and E' (see also Ref. [21]).



The fact that Eq. (4.7) is a necessary condition can be understood simply by noticing that the loss can never decrease by processing Q' through a subsequent channel, for example in the decoding operation [21]. Denoting the loss after decoherence by L_1 and the overall loss (after decoherence and decoding) by L_{12}, one has

$$0 \leq L_1 \leq L_{12} \tag{4.8}$$

showing that $L_1 = 0$ is necessary for having $L_{12} = 0$, that is for perfectly recovering decoherence by decoding.

Unlike in the classical case, it is possible to rewrite the quantum loss as a function of E' and R' only, exploiting a purely quantum feature of entropies in a tripartite system. As mentioned earlier, an important consequence of $S(R'Q'E') = 0$ is that the quantum *ternary* mutual entropy vanishes, that is

$$\begin{aligned} S(R':E':Q') &= S(R':E') - S(R':E'|Q') \\ &= S(R') + S(Q') + S(E') - S(R'Q') \\ &\quad -S(R'E') - S(Q'E') + S(R'Q'E') \\ &= 0 \end{aligned} \tag{4.9}$$

As a result, the quantum loss can be expressed as

$$L = S(R':E') \tag{4.10}$$

Therefore, a necessary and sufficient condition for perfect error correction is that the reference and the environment are statistically *independent* ($L = 0$). This condition relates entropies *after* decoherence, and thus allows us to check that, for a given code and after a specific interaction with the environment, decoherence can be recovered by decoding. As far as quantum coding is concerned, it is more useful to derive an entropic relation involving only the reference R and the codewords Q *before* unitary interaction with the environment, using some error model [*cf.* Eq. (4.5)].

C. Upper bound on the quantum loss

As before, we consider now an explicit error model in which the decoherence involves e qubits at know locations, *i.e.*, the case of e erasures. The component Q_e (of e qubits) of the codeword interacts with E while the rest Q_u (of $n - e$ qubits) remains unchanged by the interaction. Accordingly, the unitary transformation describing such an error model is $U_{RQE} = 1_R \otimes 1_{Q_u} \otimes U_{Q_eE}$. This results in the conservation rule for the mutual entropy (see Appendix A),

$$S(R':Q'_eE') = S(R:Q_eE) = S(R:Q_e) \tag{4.11}$$

where we made use of the fact that E is initially in a pure state, *i.e.*, $S(E) = 0$. This entropy can also be expressed as

$$S(R':Q'_eE') = S(R':E') + S(R':Q'_e|E') \tag{4.12}$$

by use of the chain rule for quantum mutual entropies. Using the strong subadditivity of quantum entropies,

$$\begin{aligned} S(R':Q'_e|E') = S(R'E') + S(Q'_eE') \\ -S(E') - S(R'Q'_eE') \geq 0 \end{aligned} \tag{4.13}$$

and denoting by

$$M = S(R:Q_e) \tag{4.14}$$

the initial mutual entropy (or mutual entanglement) between the reference R and the *erased* subpart Q_e of the codeword, Eqs. (4.11) and (4.12) yield an upper bound on the loss L:

$$0 \leq L \leq M \tag{4.15}$$

Consequently, if the mutual entanglement M (initial mutual entropy between R and Q_e) is zero,

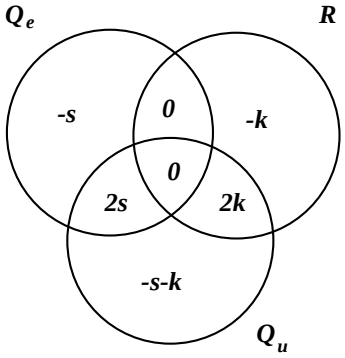
$$M = S(R:Q_e) = 0\,, \tag{4.16}$$

then the loss $L = S(R':E')$ vanishes, allowing for perfect erasure correction. In other words, the statistical independence ($M = 0$) between the reference R and the erased part of the codeword Q_e is a *sufficient* condition for perfect erasure correction, as anticipated in Eq. (4.5). Note that this condition must hold for any pattern of e erased qubits among the n qubits, a constraint which implies the quantum Singleton bound (see Section V).

The physical content of the entropic condition, Eq. (4.16), is the following. The reduced density matrix $\rho_{RQ_e} = \mathrm{Tr}_{Q_u}|\psi_{RQ}\rangle\langle\psi_{RQ}|$ obtained by tracing the state of RQ, *i.e.*, Eq. (2.2), over Q_u (ignoring the $n - e$ unchanged qubits) before decoherence must represent two *independent* systems: the k qubits of the reference R and the e erased qubits Q_e of the quantum system. The latter

e qubits can then be "erased" without interfering with R in the sense that the $n-e$ remaining qubits retain all the entanglement with R. The general entropy diagram of the joint state of the system $RQ \equiv RQ_eQ_u$ before decoherence is shown in Fig. 5 (to be compared with Fig. 2 for a classical code).

FIG. 5. Entropy diagram for a quantum erasure-correcting code. It characterizes the combined system $RQ \equiv RQ_eQ_u$ before decoherence when the condition for perfect error correction $S(R{:}Q_e) = 0$ is fulfilled. The two parameters are $S(R) = k$ and $S(Q_e) = s$.



For a code to protect an arbitrary mutual entropy between Q and R (or an arbitrary state for Q), the above condition $M = 0$ must clearly be satisfied for the worst case in which the amplitudes a_i in Eq. (2.2) are all equal ($|a_i|^2 = 2^{-k}$), that is in the case where Q and R "saturate" their entropy:

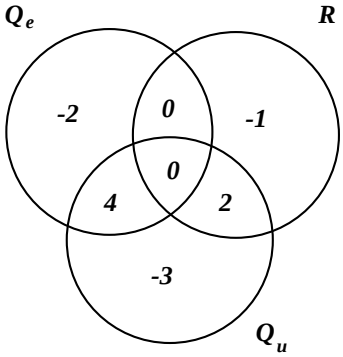
$$S(Q) = S(R) = k \tag{4.17}$$

(Note that, since $d_Q > d_L$, the entropy is limited by the size of the Hilbert space of R.) We will thus only consider this case in the following (it is important when deriving the Singleton bound on quantum codes). Because of the two constraints Eqs. (4.16) and (4.17), the ternary entropy diagram for RQ_eQ_u depends on a single unknown parameter, $s = S(Q_e)$, the entropy of the erased qubits[2]. In view of Fig. 5, we see that the e qubits of Q_e are "superfluous", as they do not yield any information about R (no mutual entanglement with R) and are thus unnecessary for recovering the original logical state. In this sense, they constitute "redundant" quantum information since the total mutual entropy $2k$ is found between R and Q_u. The unchanged qubits Q_u are entangled *separately* with the reference R ("useful" entanglement $2k$ that must be preserved by the code) and with the erased qubits Q_e ("useless" entanglement), so that any action on Q_e due to an environment E can only transfer this "useless" entanglement to E but leaves the "useful" entanglement unchanged. Indeed, if the entropy diagram Fig. 5 is achieved, then Eq. (4.15) implies that any interaction between Q_e and E necessarily results in an entropy diagram such as the one depicted in Fig. 4, where Q' is entangled *separately* with E' and R' (*i.e.*, $L = 0$), guaranteeing that one can undo decoherence by applying an appropriate decoding.

D. Example

As an illustration, we show in Fig. 6 the entropy diagram in the case of a 5 qubit code ($n = 5$) encoding $k = 1$ logical qubit with $t = 1$, *i.e.*, allowing up to $e = 2$ erasures [8,9]. The full mutual entanglement of 2 bits is found between R and Q_u, while the 2 erased qubits Q_e are independent of R. We have $S(R) = 1$, $S(Q_u) = 3$, and $S(Q_e) = 2$, so that each subsystem has the maximum allowed entropy for its Hilbert space (R, Q_u, and Q_e are made of 1, 3, and 2 qubits, respectively). Note that the 4 qubit code ($n = 4$) encoding $k = 2$ logical qubits and correcting $e = 1$ erasure [10,13] corresponds in fact to the same entropy diagram with R playing the role of Q_e and conversely. Indeed, R has then an entropy of 2 bits and shares a mutual entropy of 4 bits with Q_u (which then contains the full information about the 2 encoded qubits). This mutual entanglement is preserved against erasure of 1 qubit since Q_e is independent of R.

FIG. 6. Quantum entropy diagram of the combined system RQ_eQ_u before decoherence for the 5 bit quantum code ($n = 5$, $k = 1$, $e = 2$) [8,9].



Let us finally compare this "quantum redundancy" in the 5 qubits code with the entropic diagram characterizing a classical code. As explained in Section III, in a classical code the information (k bits) is distributed among the n bits which are then correlated with the input X in a specific way [so that Eq. (3.6) is satisfied]. Ignoring the $n-e$ unchanged bits (Y_u) leaves e bits (Y_e)

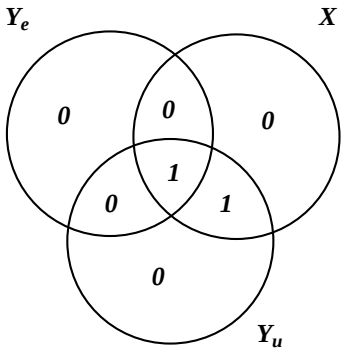
[2]The entropy diagram for a general tripartite system in a pure state depends on three parameters.

that are *redundant* [the total information is in Y_u, as implied by Eq. (3.7)], but *correlated* with the input X, in contrast with the quantum case. The entropy diagram corresponding to a simple classical code is illustrated in Fig. 7 (to be compared with Fig. 6). We consider a simple linear code with $n = 5$, $k = 2$, $e = 2$, defined in Ref. [22]

$$\begin{aligned} 00 &\longrightarrow 00000 \\ 01 &\longrightarrow 01110 \\ 10 &\longrightarrow 10101 \\ 11 &\longrightarrow 11011 \end{aligned} \tag{4.18}$$

such that the distance between any two codewords is 3 or larger. We assume that the first and the last bit are erased (Y_e), the three other ones being unchanged (Y_u), and show the entropy diagram in the case where the logical words 00 to 11 are equiprobable [the entropy in Eq. (3.3) is maximum]. The full information is found in Y_u, $H(X{:}Y_u) = 2$ bits, but the erased bits are partially correlated with X, $H(X{:}Y_e) = 1$ bit. Classical redundancy necessarily implies that the erased bits contain part of the information that is duplicated.

FIG. 7. Classical entropy diagram of XY_eY_u for the $n = 5$, $k = 2$, $e = 2$ classical linear code defined in the text.



The situation is thus quite different in a quantum code: Eq. (3.6) is replaced by its quantum counterpart Eq. (4.4), with the same physical interpretation, but the latter equation then implies the simpler condition (4.16) as a consequence of the property that the quantum ternary mutual entropy vanishes for a pure state. Such a possibility to achieve "weak" cloning through coding (in the sense that the full information is in Q_u without correlating Q_e with the reference R) is purely quantum and suggests an interesting interpretation of quantum coding, as explained in Section VI.

V. SINGLETON BOUND ON QUANTUM CODES

The above entropic considerations provide a simple way to derive the quantum analogue of the Singleton bound on error-correcting codes, obtained recently by Knill and Laflamme [11]. For a classical code, the Singleton bound (see, *e.g.*, [23]) states that the number of logical bits k than can be encoded in a code of length n recovering e erasures is such that

$$k \leq n - e \tag{5.1}$$

Of course, for a classical code recovering t errors (at unknown locations), the Singleton bound becomes

$$k \leq n - 2t \tag{5.2}$$

as a consequence of the equivalence between codes correcting t errors and $e = 2t$ erasures. In order to derive the quantum analogue of this bound, we consider the joint state of the system $RQ = RQ_eQ_u$ before decoherence. For a quantum code to protect an arbitrary entanglement between Q and R, the entropic condition $M = S(R{:}Q_e) = 0$ must is satisfied for the worst case of maximum entanglement, that is in the case where Q and R "saturate" their entropy $S(Q) = S(R) = k$. Assume for the moment that the code is such that $S(Q_e) = e$, *i.e.* that the erased qubits have the maximum entropy allowed by the dimension of the Hilbert space of Q_e. Then, the condition $M = 0$ is clearly satisfied if tracing over the $n - e$ qubits associated with Q_u yields a reduced density matrix for RQ_e that saturates its quantum entropy

$$S(RQ_e) = S(R) + S(Q_e) - S(R{:}Q_e) = k + e \tag{5.3}$$

This corresponds to the case $s = e$ in Fig. 5. Since RQ_eQ_u is in a pure state [*i.e.*, $S(RQ_eQ_u) = 0$], one has $S(RQ_e) = S(Q_u)$ by Schmidt decomposition. Expressing that the quantum entropy of Q_u is bounded from above by the logarithm of the dimension of its Hilbert space, that is $S(Q_u) \leq n - e$, one gets the inequality

$$k \leq n - 2e \tag{5.4}$$

which is the Singleton bound for quantum erasure-correcting codes. Making use of the equivalence between codes correcting errors of t qubits and the erasure of $e = 2t$ qubits, we get the Singleton bound for quantum error-correcting codes (proven in Ref. [11] for $k = t = 1$)

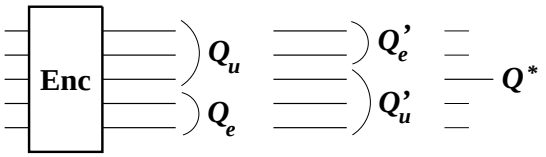
$$k \leq n - 4t \tag{5.5}$$

This condition must be satisfied by any quantum code (including degenerate codes). Mathematically, Eq. (5.4) expresses thus that it is necessary to trace over at least half of the $n + k$ qubits constituting the total entangled state $|\psi_{RQ}\rangle$ in order to open the possibility of having $k + e$ independent remaining qubits (that is which saturate their entropy), thereby allowing error correction. Eq. (5.4) suggests an interpretation of quantum coding in terms of a "weak" cloning, as explained in the next Section.

The above derivation was based on the assumption that the erased qubits have a maximum entropy, *i.e.*,

$S(Q_e) = e$. This is true for example in the case of the 5 qubit code shown in Fig. 6. However, we need to prove Eq. (5.4) in full generality, without recourse to this assumption. In general, it is possible to have $S(R{:}Q_e) = 0$ with $S(Q_e) < e$; this is the case for example when one (or more) of the physical qubits is always 0 (non-optimal code). Suppose that the condition for erasure correction $S(R{:}Q_e) = 0$ is satisfied for some pattern of e erased qubits, so that the remaining part of the codeword Q_u retains the "full" entanglement, $S(R{:}Q_u) = 2k$. The central point in deriving the quantum Singleton bound is that this entropic condition must be fulfilled for *any* pattern of e erased qubits among the n qubits. Therefore, one can choose for example another pattern of e qubits within the $n - e$ qubits that constitute Q_u, and check that they have also a vanishing mutual entropy with R.[3] Let us denote the e erased qubits in this second check by Q'_e, so that Q_u is divided into Q'_e and Q^* (the $n - 2e$ remaining qubits) as shown in Fig. 8. The corresponding entropic condition is thus $S(R{:}Q'_e) = 0$. Conversely, the unchanged qubits $Q'_u \equiv Q_e Q^*$ in this second check must also retain the full mutual entanglement with R, *i.e.*, $S(R{:}Q'_u) = 2k$. This implies that, while the e qubits of Q_e are independent of R, they must recover the total mutual entanglement $2k$ with R when supplemented only with the $n - 2e$ qubits of Q^*. These two opposite constraints must be satisfied simultaneously, which gives rise to the quantum Singleton bound.

FIG. 8. Schematic representation of the two different splittings of Q into $Q_e Q_u$ or $Q'_e Q'_u$ which are used in the derivation of the quantum Singleton bound.



In order to prove this bound, we first calculate a lower bound on the entropy of Q^*. Using the fact that $RQ = RQ_eQ'_eQ^*$ is in a pure state and the independence between Q_e and R, we have

$$\begin{aligned} S(Q_u) &= S(Q'_eQ^*) \\ &= S(RQ_e) \\ &= S(R) + S(Q_e) - S(R{:}Q_e) \\ &= k + S(Q_e) \end{aligned} \tag{5.6}$$

Then, the property of subadditivity of quantum entropies

$$S(Q'_eQ^*) \leq S(Q'_e) + S(Q^*) \tag{5.7}$$

implies the inequality

$$k + S(Q_e) - S(Q'_e) \leq S(Q^*) \tag{5.8}$$

By the same token, given the independence between Q'_e and R, we can calculate the entropy of Q'_u,

$$\begin{aligned} S(Q'_u) &= S(Q_eQ^*) \\ &= S(RQ'_e) \\ &= S(R) + S(Q'_e) - S(R{:}Q'_e) \\ &= k + S(Q'_e) \end{aligned} \tag{5.9}$$

and make use of subadditivity

$$S(Q_eQ^*) \leq S(Q_e) + S(Q^*) \tag{5.10}$$

to obtain

$$k + S(Q'_e) - S(Q_e) \leq S(Q^*) \tag{5.11}$$

Finally, combining Eqs. (5.8) and (5.11) provides a lower bound for $S(Q^*)$:

$$k \leq S(Q^*) \tag{5.12}$$

This bound is equivalent to $S(Q_eQ'_e|R) \geq 0$, and has the following interpretation. Even though Q_e and Q'_e are both independent of R, the combined system $Q_eQ'_e$ will generally be entangled with R (with a mutual entropy between 0 and $2k$). However, in contrast with the entanglement between Q_u (or Q'_u) and R, the entropy of $Q_eQ'_e$ conditional on R cannot become negative because of the opposite constraints on $S(Q_e) - S(Q'_e)$ from Eqs. (5.8) and (5.11). The quantum Singleton bound is obtained simply by noticing that $S(Q^*)$ is bounded from above by the dimension of the Hilbert space of Q^*, that is

$$S(Q^*) \leq n - 2e \tag{5.13}$$

The latter equation together with Eq. (5.12) completes the proof of Eqs. (5.4) and (5.5).

[3] This implies the simple constraint that the dimension of Q_u must be larger that the dimension of Q_e, that is $e < n - e$. This inequality, *i.e.*, the Singleton bound for $k = 1$, also results straightforwardly from the no-cloning theorem (see Section VI).

VI. DISCUSSION AND CONCLUSION

Before concluding, let us discuss the relation between the quantum no-cloning theorem and quantum erasure-correcting codes. The main point is to note that, if we can erase e qubits while being able to recover the codeword, it means that the $n-e$ remaining qubits contain all the information, so that the e qubits apparently contain a (partial) duplication of the logical word. Clearly, it is forbidden to erase half (or more) of the n qubits, since then the two halves of the codeword could be mapped on the logical word, enabling quantum cloning. Thus, one must have $n-2e>0$ (a constraint equivalent to the condition that the dimension of Q_u must exceed the dimension of Q_e). However, Eq. (5.4) is actually more restrictive, implying that it is possible to quantify the impossibility of cloning (to be more precise than a yes-or-no theorem). We will see that the Singleton bound expresses that a "weak" cloning is allowed, up to a certain extent. Let us define the number of clones (the *fractional* number of copies of the logical word) as:

$$N_c \equiv \frac{e}{n-e} \tag{6.1}$$

where the $n-e$ qubits constitute the "original" (necessary to fully recover the logical state) while the e erased qubits make the partial[4] clone. It is easy to see from Eq. (5.4) that the fractional number of clones is restricted to the range

$$0 \leq N_c \leq \frac{n-k}{n+k} \tag{6.2}$$

This somehow extends the standard no-cloning theorem to "weak" ($N_c<1$) cloning. The no-cloning theorem [15] states that it is forbidden to make one full clone, *i.e.*, $N_c \neq 1$, while Eq. (6.2) provides an upper bound on weak cloning. In the limiting case where $n=k$, the number of clones is strictly zero. This simply means that, if the codewords span the full 2^n-dimensional Hilbert space (*i.e.*, if no coding is actually used), then no cloning at all is achieved ($N_c=0$). The same is obviously true for a classical code, since, using Eq. (5.1), the equivalent condition on "weak" cloning is $0 \leq N_c \leq (n-k)/k$. When quantum coding uses only part of the Hilbert space, *i.e.*, the space of codewords is some 2^k-dimensional subspace of the full space ($k<n$), the logical states may then be viewed as partially cloned by the encoding process, the fractional number of clones being limited to $(n-k)/(n+k)$. The latter increases as a smaller subspace is used (k decreases), and tends to one (full cloning) when $n/k \to \infty$. The case $k=0$ corresponds to perfect cloning of a *fixed* (*i.e.*, non-arbitrary) pure state. Therefore, whatever the apparent "replication factor" n/k of the logical words achieved by the encoding process, the allowed number of clones $N_c<1$ (for a non-vanishing k). For a classical code, however, no such limit exists on the number of clones, as $N_c \to n/k$ when $n/k \to \infty$.

We have shown that some new insight into quantum coding can be gained by use of an information-theoretic approach paralleling the one used to describe classical coding. Such an analysis displays explicitly the similarities between classical and quantum codes, but also emphasizes the major differences. The entropic condition for a quantum erasure-correcting code is that the quantum mutual entropy between a reference and the erased part of the codeword is vanishing prior to decoherence. Such a statistical independence between the reference and the erased qubits (interacting with the environment) guarantees that the entanglement of the logical word with respect to this reference is preserved by the quantum code. This is to be compared with the corresponding entropic condition for a classical erasure-correcting code, *i.e.*, that the mutual information between the logical bits and the erased bits of the codewords, *conditional* on the remaining unchanged bits of the codewords, is vanishing. Such a classical condition, however, does *not* imply that the erased bits are independent of the logical bits. On the contrary, there must be correlations between them, and this duplication (or "cloning") of classical information is at the heart of classical codes. Such a classical redundancy has no quantum counterpart, as a consequence of the purely quantum property that the *ternary* mutual entropy vanishes for any entangled tripartite system in a pure state. In a quantum code, only a "weak" cloning is

[4]This concept of "partial" cloning is unrelated to the notion of "approximate" cloning introduced in Ref. [24]. There, a universal quantum-cloning machine is used that has two outputs being an *approximate* copy of the input. This can be viewed as two channels sharing the same input but necessarily characterized both by a *non-vanishing* quantum loss, *i.e.*, the fidelity of both copies is not one. In our case, we have two *lossless* channels: $L \to Q_u$ and $L \to Q'_u$. However, the outputs unavoidably share a common piece Q^* which cannot be reduced to zero for $S(R{:}Q_u)=2k$ and $S(R{:}Q'_u)=2k$ to hold simultaneously.

achieved, up to the extent allowed by the quantum Singleton bound, so that the erased qubits are *unentangled* with the reference although the entire codeword remains entangled with it. This reflects a major difference between classical and quantum coding.

ACKNOWLEDGMENTS

We acknowledge C. Adami and J. Preskill for very useful discussions. We thank the organizers of the ITP program on Quantum Computers and Decoherence for their invitation in Santa Barbara, where this work has been performed. This research was supported in part by the National Science Foundation under Grant Nos. PHY 94-12818, PHY 94-20470 and PHY 94-07194, and by a grant from DARPA/ARO through the QUIC Program (#DAAH04-96-1-3086).

APPENDIX A: INFORMATION-THEORETICAL FRAMEWORK FOR QUANTUM ENTROPIES

Classical information theory is centered on Shannon entropies (see, *e.g.*, [18,20]). A random variable X, distributed according to the probability distribution p_i, is characterized by the Shannon entropy

$$H(X) \equiv -\sum_i p_i \log p_i \tag{A1}$$

The Shannon entropy $H(X)$ measures the *uncertainty* of X (it vanishes if the distribution is peaked, *i.e.*, if the value of X is perfectly known). When considering two random variables X and Y, described in general by the joint probability distribution $p_{i,j}$, one can define several entropies. First, one has the joint entropy $H(XY)$, based on $p_{i,j}$ in analogy with Eq. (A1), which reflects the uncertainty of X and Y. Second, one defines the entropy of X *conditional* on Y, that is the entropy of X when Y is known (averaged over Y),

$$\begin{aligned} H(X|Y) &\equiv -\sum_{i,j} p_{i,j} \log p_{i|j} \\ &= H(XY) - H(Y) \end{aligned} \tag{A2}$$

based on $p_{i|j} = p_{i,j}/p_j$, the conditional probability of i knowing j. The equivalent definition holds for the conditional entropy of Y knowing X, *i.e.*, $H(Y|X) = H(XY) - H(X)$. Finally, one defines the *mutual* entropy between X and Y as

$$\begin{aligned} H(X{:}Y) &\equiv -\sum_{i,j} p_{i,j} \log p_{i:j} \\ &= H(X) + H(Y) - H(XY) \end{aligned} \tag{A3}$$

where $p_{i:j} = p_i p_j / p_{i,j}$ is the mutual probability of i and j. It plays the role of a mutual *information* between X and Y, that is the information about X that is conveyed by Y, or the decrease of the entropy of X due to knowledge of Y (or conversely):

$$H(X{:}Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) \tag{A4}$$

Consider now the information-theoretical description of a bipartite quantum system XY, where X and Y correspond to two quantum variables or degrees of freedom (*e.g.*, the z-component of a spin-1/2 particle). It is shown in Ref. [16,17] that a quantum information-theoretical formalism that parallels Shannon construction can be defined that is based on the von Neumann entropy, where probability distributions are replaced by density matrices, and averages are changed into quantum expectation values. We have for the quantum (von Neumann) entropy of X,

$$S(X) \equiv -\mathrm{Tr}_X(\rho_X \log \rho_X) \tag{A5}$$

where ρ_X is the density matrix characterizing the state of X. The density matrix ρ_X is obtained by a partial trace over the Y variable, *i.e.*, $\rho_X = \mathrm{Tr}_Y(\rho_{XY})$, where ρ_{XY} is the joint density matrix describing XY. A similar definition holds for $S(Y)$, based on ρ_Y. One defines then the quantum (von Neumann) *conditional* entropy,

$$\begin{aligned} S(X|Y) &\equiv -\mathrm{Tr}_{XY}(\rho_{XY} \log \rho_{X|Y}) \\ &= S(XY) - S(Y) \end{aligned} \tag{A6}$$

based on the *conditional* density matrix $\rho_{X|Y}$ (defined in [16,17]). The latter plays the role of a "quantum" conditional probability, and witnesses the appearance of non-classical correlations in the case of quantum entangled variables X and Y. Indeed, it can be shown that an eigenvalue of $\rho_{X|Y}$ can exceed one, and, consequently, that the quantum conditional entropy $S(X|Y)$ can be *negative*, a fact related to quantum non-separability (see [16,17,25]). For example, if X and Y represent two entangled quantum bits in a Bell state, we have $S(X|Y) = S(Y|X) = -1$ bit. Since negative conditional entropies are forbidden in Shannon theory, a negative value of $S(X|Y)$ obviously implies quantum non-separability, the converse being not true. On the other hand, if ρ_{XY} describes a mixture of orthogonal product states (that is a classical situation), $\rho_{X|Y}$ is then a diagonal matrix with the $p_{i|j}$'s on its diagonal, and Eq. (A6) reduces to its classical counterpart, Eq. (A2). The above definition, Eq. (A6), must therefore be viewed as a quantum *extension* of the Shannon conditional entropy in a way that incorporates quantum entanglement, while including the classical conditional entropy as a special case.

According to this, it is natural to define a quantum (von Neumann) *mutual* entropy,

$$
\begin{aligned}
S(X{:}Y) &\equiv -\mathrm{Tr}_{XY}(\rho_{XY}\log\rho_{X:Y}) \\
&= S(X)+S(Y)-S(XY) \\
&= S(X)-S(X|Y) = S(Y)-S(Y|X) \qquad \text{(A7)}
\end{aligned}
$$

based on the *mutual* density matrix $\rho_{X:Y}$ (defined in [16,17]). The interpretation is the same as in Shannon information theory, and $S(X{:}Y)$ is a symmetric quantity. Subadditivity of quantum entropies, *i.e.*, $S(XY) \leq S(X)+S(Y)$, implies that $S(X{:}Y) \geq 0$, just as for Shannon mutual entropies. However, in the case of quantum entangled variables, $S(X{:}Y)$ can reach twice the maximum allowed value in Shannon theory [16,17]:

$$
S(X{:}Y) \leq 2\min[S(X), S(Y)] \qquad \text{(A8)}
$$

For instance, we have $S(X{:}Y) = 2$ bits between the members of an EPR pair. Note that $S(X{:}Y)$ is not a *measure* of entanglement in the sense that it can be non-zero for classical (separable) mixtures. It does not necessarily exceed the classical upper bound, $\min[S(X), S(Y)]$, for quantum entangled systems. Thus, $S(X{:}Y)$ is rather a quantum mechanical extension of the usual Shannon mutual entropy, which measures quantum as well as classical correlations. Nevertheless, it plays an important role in the information-theoretic description of quantum channel and error correction, as emphasized throughout this paper (see also [21]).

Consider a quantum system X entangled with a reference R, so that the joint system RQ is in the pure state $\sum_i \sqrt{p_i}|i_R\rangle|i_X\rangle$. The system X is sent through a quantum channel (which does not act on R). It is easy to see that, if the channel (including error-correction) is "perfect", *i.e.*, if the output Y ends up in a joint pure state (together with R) such that the quantum mutual entropy with R is conserved, then an *arbitrary* quantum state is preserved in the channel[5]. Indeed, as R is unchanged, any joint state of RY that is characterized by $S(R{:}Y) = S(R{:}X)$ and $S(RY) = S(RX) = 0$ is necessarily of the form $\sum_i \sqrt{p_i}|i_R\rangle(U|i_X\rangle)$ where U is a *fixed* unitary transformation (it does *not* depend on the p_i's). Thus, up to a given change of basis, the output Y is in the same entangled state with R. Projecting R onto any pure state shows that the corresponding pure state of X (the "relative" state) has been preserved, *i.e.*, Y ends up in the same state.

Another important property of the quantum mutual entropy $S(X{:}Y)$ is that it is conserved when the bipartite system XY undergoes a unitary transformation of the form $U_X \otimes U_Y$. Indeed, if

$$
\rho'_{XY} = (U_X \otimes U_Y)\rho_{XY}(U_X \otimes U_Y)^\dagger \qquad \text{(A9)}
$$

then $\rho'_X = \mathrm{Tr}_{Y'}(\rho'_{XY}) = U_X \rho_X U_X^\dagger$ and similarly for ρ'_Y, so that

$$
S(X'{:}Y') = S(X{:}Y) \qquad \text{(A10)}
$$

follows from Eq. (A7) together with the conservation of von Neumann entropy under a unitary transformation. In particular, any entangled system XY that undergoes a local operation separately on X and Y retains its initial entanglement between X and Y, *i.e.*, $S(X{:}Y)$ is conserved. This property is useful in the context of quantum channels and quantum error correction.

The quantum information-theoretical formalism defined above can be generalized to multipartite systems, in analogy to the Shannon construction [16,17]. The definition of the conditional (and mutual) density matrices provides grounds for the quantum extension of the usual algebraic relations between Shannon entropies (see, *e.g.*, [18,20]). The resulting framework for quantum information theory goes beyond classical correlations, *i.e.*, accounts for situation where n quantum variables are entangled, by allowing conditional entropies to be negative. Of course, it also includes Shannon theory as a special case. Consider, for example, a tripartite quantum system XYZ. First, one can write the *chain rule* for quantum entropies,

$$
S(XYZ) = S(X) + S(Y|X) + S(Z|XY) \qquad \text{(A11)}
$$

One can also define the von Neumann *conditional mutual* entropy,

$$
\begin{aligned}
S(X{:}Y|Z) &= S(X|Z) - S(X|YZ) \\
&= S(X|Z) + S(Y|Z) - S(XY|Z) \\
&= S(XZ) + S(YZ) - S(Z) - S(XYZ) \qquad \text{(A12)}
\end{aligned}
$$

which reflects the quantum mutual entropy between X and Y, when Z is known. Eq. (A12) follows the definition of a mutual entropy, Eq. (A7), but with all entropies being conditional on Z. Just like with classical entropies, the property of *strong subadditivity* of quantum entropies holds, that is $S(X{:}Y|Z) \geq 0$. Conditional

[5]The classical analogue of this property is intuitive. If the input X of a classical channel is copied into a memory M (so that M is thus perfectly correlated with X), the correlation between the output Y and the memory M reflects the "quality" of the channel. In particular, if the mutual entropy between Y and M is equal to that between X and M, then the classical channel is perfect (lossless).

mutual entropies are also used in the quantum analogue of the chain rules for mutual entropies, that is

$$S(X{:}YZ) = S(X{:}Z) + S(X{:}Y|Z) \tag{A13}$$

Finally, the relation between conditional and mutual entropies, $S(X) = S(X|Z) + S(X{:}Z)$ can be extended to a tripartite system, that is

$$S(X{:}Y) = S(X{:}Y|Z) + S(X{:}Y{:}Z) \tag{A14}$$

so that we can split $S(X{:}Y)$ into a conditional piece and a mutual piece with Z. The latter piece, $S(X{:}Y{:}Z)$, characterizes therefore the *ternary* mutual entropy, *i.e.*, that piece of the mutual entropy between X and Y that is also shared by Z. All these relations between entropies can be understood very easily using Venn diagrams [16,17,21].

Finally, an important property of *quantum* entropies which has no classical counterpart, is that, for any entangled tripartite system XYZ in a pure state, the ternary mutual entropy vanishes [17], *i.e.*,

$$\begin{aligned} S(X{:}Y{:}Z) &= S(X) + S(Y) + S(Z) - S(XY) \\ &\quad -S(XZ) - S(YZ) + S(XYZ) \\ &= 0 \end{aligned} \tag{A15}$$

This results from the fact that $S(XYZ) = 0$ implies $S(XY) = S(Z)$, $S(XZ) = S(Y)$, and $S(YZ) = S(X)$, as a consequence of the Schmidt decomposition of the state of XYZ.

[1] S. Lloyd, Science **261**, 1569 (1993).
[2] D.P. DiVincenzo, Science **270**, 255 (1995)
[3] A. Ekert and R. Jozsa, Rev. Mod. Phys. **68**, 733 (1996).
[4] P.W. Shor, Phys. Rev. A **52**, 2493 (1995).
[5] A. Steane, Phys. Rev. Lett. **77**, 793 (1996).
[6] A.R. Calderbank and P.W. Shor, Phys. Rev. A **54**, 1098 (1996).
[7] A. Ekert and C. Macchiavello, Phys. Rev. Lett. **77**, 2585 (1996).
[8] R. Laflamme, C. Miquel, J.P. Paz, and W.H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).
[9] C.H. Bennett, D.P. DiVincenzo, J. A. Smolin, and W.K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[10] L. Vaidman, L. Goldenberg, and S. Wiesner, Phys. Rev. A **54**, R1745 (1996).
[11] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997)
[12] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane, Report No. quant-ph/9608006.
[13] M. Grassl, T. Beth, and T. Pellizzari, Report No. quant-ph/9610042.
[14] A. Peres, Report No. quant-ph/9611046.
[15] W.K. Wootters and W.H. Zurek, Nature **299**, 802 (1982); D. Dieks, Phys. Lett. **92A**, 271 (1982).
[16] N.J. Cerf and C. Adami, Report No. quant-ph/9512022; N.J. Cerf and C. Adami, in Proc. of 2nd Int. Symp. on Fundamental Problems in Quantum Physics, edited by M. Ferrero and A. van der Merwe (Kluwer Academic Publishers, Dordrecht, 1997); also in Report No. quant-ph/9610005.
[17] N.J. Cerf and C. Adami, Report No. quant-ph/9605002; N.J. Cerf and C. Adami, in Proc. of 4th Workshop on Physics and Computation, edited by T. Toffoli *et al.* (New England Complex Systems Institute, Cambridge, MA, 1996); also in Report No. quant-ph/9605039.
[18] R.B. Ash, *Information Theory* (Dover, New York, 1965).
[19] B. Schumacher, Phys. Rev. A **54**, 2614 (1996); B. Schumacher and M. A. Nielsen, Phys. Rev. A **54**, 2629 (1996).
[20] T.M. Cover and J.A. Thomas, *Elements of Information Theory* (Wiley, New York, 1991).
[21] C. Adami and N.J. Cerf, Report No. quant-ph/9609024.
[22] R. Cleve, Report No. quant-ph/9612048.
[23] J.H. van Lint, *Introduction to Coding Theory*, (Springer-Verlag, Berlin, 1992).
[24] V. Buzek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
[25] N.J. Cerf and C. Adami, Phys. Rev. A **55**, 3371 (1997).